AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The image of iPhone XR, serial number F17YJ82BKXKP, currently located at 3055 Kettering Boulevard, Suite 205, Dayton, Ohio 45439

Case No. 2:19-mj-536

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1001	Making false statements
18 U.S.C. § 1343	Wire fraud
18 U.S.C. § 287	Making a false or fraudulent claim against the U.S.

The application is based on these facts:

See Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Delia McMullen Special Agent
Applicant's signature

Printed name and title

Sworn to before me and signed in my presence.

Date: July 9, 2019

Judge's signature

City and state: Columbus, OH

Elizabeth Preston Deavers, Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF THE **IMAGE OF iPHONE XR, SERIAL NUMBER F17YJ82BKXKP**, CURRENTLY LOCATED AT **3055 KETTERING BOULEVARD, SUITE 205, DAYTON, OHIO 45439**

Case No. 2:19-mj-536

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, **Delia McMullen**, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—the image of an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Defense Criminal Investigative Service (DCIS), which is part of the Office of the Inspector General for the U.S. Department of Defense (DoD). I have been so employed for approximately 16 years. In my current capacity, I am charged with investigating acts of suspected DoD contract fraud.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is an image of an iPhone XR, serial number F17YJ82BKXKP. The actual iPhone XR, serial number F17YJ82BKXKP was not seized and left with the original owner; an image of the iPhone XR, serial number F17YJ82BKXKP was made and copied to Seagate hard drive, serial number Z520J6T1. From hereinafter, the image of the iPhone XR, serial number F17YJ82BKXKP contained Seagate hard drive, serial number Z520J6T1 will be referred to as the "Device." The Device is currently located at 3055 Kettering Boulevard, Suite 205, Dayton, Ohio 45439.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

Contracting Process

6. The United States Department of Defense (DoD), contracts through its various agencies, such as the Defense Logistics Agency (DLA). DLA is the United States' combat logistics support agency, and as such manages the global supply chain for all military services, 10 combatant commands, other federal agencies, and partner and allied nations. DLA has three primary depots that manage the military's global supply chain – DLA Land and Maritime (L&M) in Columbus, Ohio, DLA Aviation in Richmond, Virginia, and DLA Troop Support (TS) in Philadelphia, Pennsylvania.

7. When the DoD determines that a particular part is needed, the DoD issues "Solicitations," or Requests for Quotation (RFQs) electronically through a web-based application, DIBBS (DLA's Internet Bid Board System). Users (potential contractors) are able

to search for, view, and submit secure quotes based upon the RFQs for the items DLA is looking to obtain. The solicitations (RFQ's) list the DoD requirements, which can include specified manufacturers and part numbers, drawings and/or specifications such that any potential contractor is aware of exactly how the part is to be made or where they can obtain the part. DoD contractors are required to have a quality control system in place to insure the parts supplied to the DoD are in accordance with DoD drawings and specifications. In addition to noting the contractor's agreement or disagreement with the requirements of the solicitation, the quote, or bid, submitted will list the contractor name, business location and an email address.

8. In order to conduct business with the DoD, contractors must register in the System for Award Management (SAM), to include providing an email address, and agree to receive payments electronically. The contractors must also obtain a Commercial and Government Entity (CAGE) code. The CAGE code is a 5-character identification number used extensively within the federal government, assigned by the DLA. The CAGE code is used to support a variety of mechanized systems throughout the government and provides a standardized method of identifying a given contractor facility at a specific location.

9. In the contracting process, once parts are shipped to the DLA, contractors enter the shipping and invoicing information electronically, through a secure, web-based system, which allows the government to receive and pay electronically. Upon receiving the invoice, which also represents that the contractor is providing goods in conformance with the contract requirements, the DoD, through the Defense Finance and Accounting Service (DFAS), Columbus, Ohio; in the Southern District of Ohio, will issue electronic payment to the supplying contractor and retain a voucher as a record of the payment.

10. DLA L&M in Columbus is also home to laboratories used to test and identify nonconforming parts sold to DLA, including the capability to test for counterfeit material, substitute inferior products, and remark/over brand items. These laboratories at DLA L&M are used to test all suspect parts provided to DLA worldwide.

Terrell-MMPEDistributors LLC

11. **Terrell-MMPEDistributors LLC** was formed in Illinois on June 29, 2014. The Principle Address and Agent Street Address provided to the State for the company was 18534 Oak Avenue, Lansing, IL 60438. The Agent name filed with the State was **Carol Terrell.** On March 1, 2013, **Terrell-MMPEDistributors** was initially registered in the SAM. The current record maintained in the SAM indicates the physical and mailing address is 18534 Oak Avenue, Lansing, IL 60438 and listed **Carol Terrell** under the "Tax Payer Name", "Name of Individual Executing Consent", "Signature" and "Remittance Name" sections and listed an email address maj.mot.pacifelect@gmail.com. From March 1, 2013 through November 12, 2018, approximately 28 modifications of **Terrell-MMPEDistributors'** information in the SAM were made, including annual re-registrations of the company in the SAM. The initial registration indicated **Carol Terrell** as the "D&B Legal Business Name", "Doing Business As: Major Motor & Pacific Electric Distributors." The current record indicates **Terrell-MMPEDistributors** as the "D&B Legal Business Name", "Doing Business As: MMpedistrib". In both **Terrell-MMPEDistributors** initial registration in the SAM and all subsequent modifications, **Carol Terrell** was identified as "Tax Payer Name", "Name of Individual Executing Consent", Signature" and "Remittance Name" of **Terrell-MMPEDistributors.** On March 8, 2013, **Terrell-MMPEDistributors** registered and established a CAGE Code. A check of the CAGE

Program database identified contact information, Point of Contact as **Carol Terrell**, address 18534 Oak Avenue, Lansing, IL 60438.

12. Since 2015, **Terrell-MMPEDistributors** has received approximately $549,000 in DLA contracts.

13. **Carol Terrell** and **Terrell-MMPEDistributors** came to the attention of DLA L&M in December 2018 after DLA L&M conducted testing on parts pulled from stock on four different contracts, received by **Terrell-MMPEDistributors**; all parts failed the tests. These four contracts are valued at approximately $59,000. These parts consisted of engine cooling system pumps, piston rings, engine oil pump assemblies and cooling system pumps used on U.S. military vehicles, including the Mine Resistant Ambush Protected Vehicles, Heavy Expanded Mobility Tactical Truck, Cargo Trucks and Armor Wrecker Trucks. DCIS subsequently opened a criminal investigation into **Terrell-MMPEDistributors** and **Carol Terrell**.

14. DLA L&M identified additional parts received from **Terrell-MMPEDistributors** on eight separate contracts valued at $55,173, which were in DLA L&M stock. DLA L&M pulled and tested these parts as well; all parts failed the tests. These parts consisted of engine lubricating oil coolers, power supplies, piston connecting rods, exhaust mufflers, cooling system pumps, and gaskets used on U.S. military weapon systems and vehicles, including the DDG-1000 Zumwalt Class Destroyer, Littoral Combat Ship, Heavy Expanded Mobility Tactical Truck, and the U-2 Airframe.

15. The above twelve contracts, which were issued by DLA L&M to **Terrell-MMPEDistributors** during September 24, 2015 through June 6, 2017, and on which **Terrell-MMPEDistributors** sold parts to DLA L&M that ultimately failed the tests and could not be used on the intended U.S. military weapon systems or vehicle, were "code and part" contracts.

Contracts issued by DLA are typically one of two types of contracts: "drawing" contracts or code and part contracts. On a drawing contract, the contractor is required to manufacture a specific part in accordance with specifications identified by DLA in its solicitation and contract. On a code and part contract, the contractor is required to provide DLA a specific part that was manufactured by an approved source; DLA identifies the specific part and approved source(s) in its solicitation and contract. All of the above twelve DLA contracts with DLA were code and part contracts. **Terrell-MMPEDistributors** was required to provide DLA specific parts manufactured by approved sources, but instead sold inferior parts from unapproved sources.

16. For example, one of the DLA L&M contracts was for seven power supplies to be used on the Littoral Combat Ship. DLA L&M was able to obtain four and noted that all four of the power supplies have visual signs on the mounting brackets of previous use. It was determined that besides visual signs of previous use, the units were out of warranty, the serial numbers were from 2000, 2002, and some perhaps from 1997. DLA L&M determined the power supplies provided by **Terrell-MMPEDistributors** were old stock, possibly used and unacceptable for use. The parts provided by **Terrell-MMPEDistributors** were not what the parts **Terrell-MMPEDistributors** certified they would provide under the conditions of the contract.

17. In its bids for the above 12 contracts, **Terrell-MMPEDistributors** certified to DLA that it would provide the correct part from an approved source. Each quote contains the following "Quoter" information:

> Name: **Terrell-MMPEDistributors, LLC.**
> Phone: (800)760-7941
> Email: Maj.mot.pacifelect@gmail.com

18. A query in the CLEAR database on the above phone number revealed that this phone number comes back to **Carol Terrell**.

19. A review of DFAS records for the above 12 contracts revealed **Terrell-MMPEDistributors** electronically invoiced DFAS for payment of these contracts and that DFAS in fact electronically paid **Terrell-MMPEDistributors** based upon the invoice **Terrell-MMPEDistributors** submitted. For example, **Terrell-MMPEDistributors** bid without exception on June 20, 2016 to provide 65 Engine Cooling System Pumps, used on or in support of Mine Resistant Ambush Protected Vehicles. **Terrell-MMPEDistributors** was awarded the contract, in the amount of $18,850.00, on June 21, 2016. **Terrell-MMPEDistributors** electronically invoiced DFAS for payment for this contract on September 7, 2016 and received electronic payment by DFAS in the amount of $18,850.00 on September 23, 2016.

20. Based on your Affiant's prior knowledge, training and experience, as well as the evidence gathered to date in this investigation, I know that it is common and typical for owners and managers of small businesses engaging in U.S. Government contracting to maintain business records that are in electronic format and can be accessed, saved or otherwise memorialized on computers, wireless telephones or other computer devices. For example, the contracting process with DoD generates documents such as a solicitation, bid or quote, the contract or purchase order itself and documents related to the invoicing of the DoD for payment. These documents can all be completed and accessed online, and saved electronically as well. Contracting process notifications also are sent via electronic mail. Based upon my experience and the experience of other law enforcement agents, it is common for individuals to use their wireless telephones similar to how one uses a computer by using email features, accessing and logging-on to websites, internet search features, imputing calendar events and notes, and other features of the

wireless telephone used in daily life and business. As such, I would submit there is probable cause to issue a search warrant for the Device.

21. The Device is currently in the lawful possession of the Defense Criminal Investigative Service (DCIS). The Device was seized on June 18, 2019 during the execution of a federal search warrant authorizing agents to seize "computers or storage media…" The Device came into the DCIS' possession under the belief that a wireless telephone, especially an iPhone which is similar to a computer or storage media, was within the purview and authority of the warrant originally executed on June 18, 2019. Therefore, while it is believed that the DCIS may already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device, which was not named specifically in the original warrant, will comply with the Fourth Amendment and other applicable laws.

22. The Device is currently in storage at 3055 Kettering Boulevard, Suite 205, Dayton, Ohio 45439. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the DCIS.

TECHNICAL TERMS

23. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication

through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

24. Based on my training, experience I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

25. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual

information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

27. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

28. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

29. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Delia McMullen
Special Agent
Defense Criminal Investigative Service

Subscribed and sworn to before me
on July 8, 2019:

Honorable Elizabeth Preston Deavers
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is an image of an iPhone XR, serial number F17YJ82BKXKP. The actual iPhone XR, serial number F17YJ82BKXKP was not seized and left with the original owner; an image of the iPhone XR, serial number F17YJ82BKXKP was made and copied to Seagate hard drive, serial number Z520J6T1. From hereinafter, the image of the iPhone XR, serial number F17YJ82BKXKP contained Seagate hard drive, serial number Z520J6T1 will be referred to as the "Device." The Device is currently located at 3055 Kettering Boulevard, Suite 205, Dayton, Ohio 45439.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

All records and information on the Device described in Attachment A that relate to violations of Title 18, United States Code, Sections 1001 (making false statements), 1343 (wire fraud), and 287 (making a false or fraudulent claim against the U.S), those violations involving **Carol Terrell, Terrell-MMPEDistributors LLC**, and other known and unknown persons and companies, and occurring after March 1, 2013, including:

a) Information related to U.S. Department of Defense (DoD) contracting, to include but not limited to, solicitations, bids/quotes, purchase orders/contracts, DFAS or other payment records, inspection records or results including any drawings or certifications whether conducted in-house or by a government agency such as DCMA or a private third-party; traceability documents or requests for traceability; the ordering or manufacturing of any parts provided to the DoD including any receipts, invoices, correspondence with suppliers; the shipping of parts from suppliers and to the DoD.

b) Information related to the creation, ownership, registration, corporate meeting minutes, tax records and annual reports, employees or dissolution of **Terrell-MMPEDistributors LLC**; the extent of their dealings with the DoD and any of its agencies to include any records of CAGE code or SAM applications or registrations, pre-award survey documents, quality manuals and correspondence with DoD;

c) Records and information relating to fraud committed against the DoD and any of its agencies;

d) Records and information relating to the use of e-mail accounts;

e) Evidence of who used, owned, or controlled the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

f) Evidence of software that would allow others to control the Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

g) Evidence of the lack of such malicious software;

h) Evidence indicating how and when the Device was accessed or used to determine the chronological context of Device access, use, and events relating to crime under investigation and to the Device user;

i) Evidence indicating the Device user's state of mind as it relates to the crime under investigation;

j) Evidence of the attachment to the Device of other storage devices or similar containers for electronic evidence;

k) Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device;

l) Evidence of the times the Device was used;

m) Passwords, encryption keys, and other access devices that may be necessary to access the Device;

n) Records of or information about Internet Protocol addresses used by the Device;

o) Records of or information about the Device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

p) Contextual information necessary to understand the evidence described in this attachment.